device to its owner if the owner's identity and contact information are unknown. Similarly, if a stolen device is recovered by a law enforcement agency, the law enforcement agency will generally consider owner identification an essential part of any effort to reunite the device and the owner.

Conventional approaches to solving the return-to-owner problem include such things as nametags, labels affixed to the device, and various forms of engraved indicia. Nametags and labels are common, well known, cheap, and simple to employ. However, nametags can be removed easily. The removal may be either intentional or inadvertent but the result is the same, i.e., a device with an unidentifiable owner. Labels affixed to the device either through the use of adhesives or other means can also be removed. Even if removal is not easily accomplished, often nametags and labels can be rendered unreadable by environmental conditions to which the portable device is subjected during normal use. Engraving offers a more permanent means of owner identification. Unfortunately, the very permanence of engraving makes changing ownership inconvenient. For example, if the owner of a device wishes to sell the device, engraved indicia can pose a complication for updating the proper identification of the new owner. In addition to the problem of updating ownership identification, engraving often requires that the device housing be partially defaced, an act that may decrease the esthetic qualities and resale value of the device.

Thus, a portable electronic device having a security lockout feature, which both disables the device to deny use to an unauthorized user and simultaneously provides for an identification of the rightful owner, fulfills a long-felt need in the area of portable electronic devices. Advantageously, such a security lockout feature facilitates the return of the lost or stolen electronic device to its rightful owner and further, also provides for updating and changing the ownership identification and contact information if and when the ownership of the device legitimately changes.

The present invention is a method of return-to-owner security lockout for an electronic device and a portable electronic device having return-to-owner security lockout. According to the present invention, a portable electronic device is disabled if a valid lockout bypass input is not received. The security lockout of the present invention effectively prevents the use of the electronic device by other than an

authorized user. Moreover, when the device is disabled, an interface on the electronic device is employed by the present invention to display owner information. The displayed owner information facilitates the return of a lost or stolen portable device to its rightful owner. Furthermore, the authorized user or the owner can update the owner information when the device is not disabled.

In one aspect of the present invention, a method 100 of return-to-owner security lockout for a portable electronic device is provided. A flow chart of the method 100 of the present invention is illustrated in Figure 1. The method 100 comprises receiving 110 a lockout bypass input and comparing 120 the received lockout bypass to a lockout bypass template or expected input to determine whether or not the lockout bypass is valid.

The lockout bypass is an input to the electronic device that enables an authorized user to be unambiguously identified by the device. In other words, the lockout bypass is essentially unique to the authorized user. Any type of unique input can be used as the lockout bypass including, but not limited to, a password, a personal identification number (PIN), a coded radio frequency (RF) or infrared (IR) signal, a bar code scan, a retinal scan, a fingerprint scan, and a key (including a magnetic strip key card) that is inserted into the device. One skilled in the art is familiar with many other such means for unambiguously or uniquely identifying an authorized user to an electronic device, all of which are within the scope of the present invention.

For example, consider a lockout bypass comprising a password or equivalently a personal identification number (PIN). A password or PIN unique to the user is employed as a means of identifying the user to the device employing the method 100. As used in conjunction with the present invention, the password or PIN serves as an unambiguous means of identification in a manner that is entirely analogous to the use of a password in conjunction with various computer system accounts, bank accounts, and credit card accounts.

Continuing with the password or PIN lockout bypass example, the step of receiving 110 a lockout bypass input comprises issuing a request for a password. Typically, the device utilizing the method 100 issues the request. In some embodiments, the authorized user knows that a lockout bypass input is necessary to

enable the device. Therefore, the step of issuing a request for the lockout bypass input is considered optional for the present invention. The step of receiving 110 further comprises entering or inputting the password. The password can be entered into the device in many ways. Typically, the user enters the password into the device using a user interface of the device.

According to the password lockout bypass example, the step of comparing 120 compares the entered password to a password template stored in memory of the device. In some cases, the password is encoded or encrypted prior to the step of comparing 120. In such cases, the encoded password is compared to a similarly encoded password template stored in memory. If, during the step of comparing 120, the entered password matches or otherwise corresponds to the stored password template, the lockout bypass input is considered to be valid. If the passwords do not match or correspond, the bypass input is considered to be invalid.

The password can be input using the user interface provided by the electronic device in a manner familiar to one skilled in the art. For example, if the device provides keys or buttons, pressing the keys in an appropriate sequence may be used to enter the password or PIN. Alternatively, a 'verbal' password can be used in devices with voice recognition. In this alternative, the password may be spoken by the user as a means of inputting the password.

In another example, the step of receiving 110 the lockout bypass input comprises inserting a key into the device. The key has a unique characteristic, such as an encoded magnetic strip on a card or a mechanical pattern of grooves, ridges, and/or holes, that is recognizable by the device. A key, such as that used for an automobile ignition system, is one example of such a key. In this example, the step of comparing 120 compares the inserted key to a key template. If a correct key is inserted into the device, the comparison 120 determines that the lockout bypass input is valid. If a key is not inserted or an incorrect key is inserted, the lockout bypass input is considered to be invalid. In this example of the step of receiving 110, the key may remain inserted during device operation or the key may be removed once the step of comparing 120 is completed.